

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 11-283326

(43)Date of publication of application : 15.10.1999

(51)Int.Cl.

G11B 20/10
H04L 9/26

(21)Application number : 10-100436

(71)Applicant : KOKUSAI JOHO KAGAKU
KENKYUSHO:KK
VICTOR CO OF JAPAN LTD

(22)Date of filing : 27.03.1998

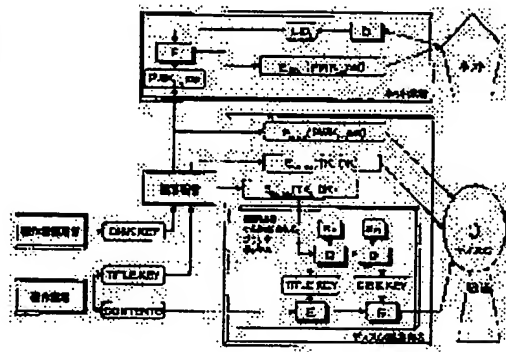
(72)Inventor : KO SHINU
HIRATA ATSUMI

(54) CONTENTS INFORMATION TRANSMITTING METHOD AND DEVICE

(57)Abstract:

PROBLEM TO BE SOLVED: To reduce the cost of a reproducer and to obtain a ciphering system capable of being used commonly between media by performing decodings of plural kinds of information recording media including ciphered contents information and plural kinds of information recording media including decoding key information with a single method.

SOLUTION: A title key TK and a disk key DK to be determined by a copyright holder and a copyright manager are ciphered to EKa, EKb (TK, TD) with master keys Ka, Kb by a key manager and also they are ciphered to EKp, EKq (TK, DK) by master keys Kp, Kq for disk production. A disk manufacture chipfers contents information in two steps by the TK, TD decoded in a black box to record them on a disk. Besides, the manufacture records the EKa, EKb (TK, TD), Ka, Kb ciphered by a maker's ID key and the player work key set ciphered by a user's ID key on the disk.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

Copyright (C); 1998,2003 Japan Patent Office

*** NOTICES ***

Japan Patent Office is not responsible for any damages caused by the use of this translation.

1. This document has been translated by computer. So the translation may not reflect the original precisely.
2. **** shows the word which can not be translated.
3. In the drawings, any words are not translated.

CLAIMS

[Claim(s)]

[Claim 1] The contents communication-of-information method characterized by performing the informational decryption by which encryption was carried out [aforementioned] by the single method in the contents communication-of-information method including the decryption key information including the enciphered contents information which decrypts two or more the information record media and the contents information by which encryption was carried out [aforementioned] on a seed one or more of transmitting two or more information record media of a seed to a user one or more.

[Claim 2] The information record medium of two or more sorts of one not less than which contain two or more decryption keys further enciphered by other encryption keys in the decryption key including the enciphered contents information which decrypts the information record medium of a seed, and the contents information by which encryption was carried out [aforementioned] one or more, And the contents communication-of-information method characterized by performing the informational decryption by which encryption was carried out [aforementioned] by the single method in the contents communication-of-information method containing the user ID key which decrypts the decryption key by which encryption was carried out [aforementioned] of transmitting two or more information record media of a seed one or more.

[Claim 3] The contents communication-of-information method according to claim 1 or 2 characterized by for at least one of the aforementioned encryption being enciphered by two stages by two kinds of keys, and at least one of the aforementioned decryptions being decrypted by two stages by two kinds of keys.

[Claim 4] The contents communication-of-information method according to claim 1 or 2 characterized by for at least one of the aforementioned encryption being enciphered by two stages by two kinds of keys using chaos cryptography, and the aforementioned decryption being decrypted by two stages by two kinds of keys.

[Claim 5] The contents information transfer system characterized by performing [two or more] the informational decryption by which encryption was carried out [aforementioned] with a specific means in the contents information transfer system including the decryption key information including the enciphered contents information which decrypts an information record means of communication and the contents information by which encryption was carried out [aforementioned] on a seed equipped with two or more information record means of communication of a seed one or more one or more.

[Claim 6] The information record means of communication of two or more sorts of one not less than including the enciphered contents information, The information record means of communication of two or more sorts of one not less than containing the decryption key further enciphered by other encryption keys in the decryption key which decrypts the contents information by which encryption was carried out [aforementioned], And it sets to two or more sorts containing the user ID key which decrypts the decryption key by which encryption was carried out [aforementioned] of contents information transfer systems equipped with two or more information record means of communication of a seed one or more. The contents information transfer system characterized by performing the informational decryption by which encryption was carried out [aforementioned] with a specific means.

[Claim 7] The contents information transfer system according to claim 5 or 6 characterized by having a means by which at least one of the aforementioned encryption is enciphered by two stages by two kinds of keys, and a means by which at least one of the aforementioned decryptions is decrypted by two stages by two kinds of keys.

[Claim 8] The contents information transfer system according to claim 5 or 6 characterized by having a means by which at least one of the aforementioned encryption is enciphered by two stages by two kinds of keys using chaos cryptography, and a means by which the aforementioned decryption is decrypted by two stages by two kinds of keys.

[Translation done.]

* NOTICES *

Japan Patent Office is not responsible for any damages caused by the use of this translation.

1. This document has been translated by computer. So the translation may not reflect the original precisely.
2. **** shows the word which can not be translated.
3. In the drawings, any words are not translated.

DETAILED DESCRIPTION

[Detailed Description of the Invention]

[0001]

[The technical field to which invention belongs] this invention relates to encryption of the key which enciphers the contents information and contents information in an information transmission.

[0002]

[Description of the Prior Art] Radio broadcasting and communication media, such as wire communication media, such as package media, such as a disk and a tape, and a network, ground broadcast, satellite broadcasting, and communication, are used as a means of communication in telling contents information etc. conventionally. As for the contents information sent using these media, peculiar encryption processing (scramble processing) is performed according to each medium.

[0003] For example, it is unreproducible as long as there will be no key which decrypts data even if it reads the recorded data or copies, if the contents information recorded on the disk is data with which image information was enciphered. The operation which neither the illegal copy of a disk nor a copyright person means by such encryption is prevented.

[0004] Although code release processing is usually performed in many cases using exclusive use LSI, it is also possible to carry out by software by the general purpose computer. However, even though it takes which method, it is required to prevent from analyzing using a debugger, an assembling tool, etc. The software equipped with the "resistance" which prevents such internal analysis is called tamper resist software (Tamper Resistant Software).

[0005] The outline of an example of the contents information encryption in a disk is shown in drawing 1. Contents information is enciphered combining the master key which the key manager in a neutral position holds, and the title key which the disk key and those [copyright] whom a copyright person etc. sets manage hierarchical.

[0006] A master key is a different encryption key for every LSI for code release, or decryption software maker. A key manager manages these master keys collectively. Copyright managers, such as a movie company and a concert company, manage a disk key, and a copyright manager manages a title key instead of a copyright person or a copyright person. One disk key may be set as one disk, and the multi-statement of the title key may be carried out according to every title and a copyright person. A disk key is enciphered using a master key. When decrypting by exclusive use LSI, key data, an algorithm, etc. are concealed by the internal structure of LSI.

[0007] When enciphering a disk key, the disk key set which can also decrypt the master key with which it differed for every LSI maker is made, and it records on the disk. The title key enciphered by the disk key enciphered with the enciphered master key and the disk key is recorded on a disk with the contents information enciphered by the title key. Since any key is enciphered, a title key required for a decryption of contents information cannot be known.

[0008]

[Problem(s) to be Solved by the Invention] When a disk and a code key are sent for contents information by communication, encryption is made in many cases by the respectively original method, and two or more kinds of decryption processings must be prepared. For this reason, since a regenerative apparatus is equipped with two or more sorts of decryption meanses, equipment is complicated and cost goes up. Moreover, if equipment is simplified, a problem will come out in respect of the safety of a code.

[0009] As shown in drawing 1, in the cipher system of the conventional disk, it is a title key about contents information, is a disk key about a title key, and is the serial-pattern of enciphering a disk key with a master key, respectively. Since it can decode by within a time [limited] when a limit has especially the length of a key if the unjust decode person of a code attacks by the method of "total key search" only to a title key, safe intensity is completely insufficient. For example, if a code key becomes 40 bit, since it is decipherable within several hours, copyright cannot be protected effectively. Moreover, since a master key will be stored in a player as it is, it may be searched by the decode person and is very dangerous with the conventional cipher system.

[0010] The cipher system used by the disk system has information, such as three encryption key data, and these decryption algorithms, algorithms of path authentication. In order to protect such confidential information from reverse engineering, it is necessary to cope with software, a debugger, snapshot analysis, a setup of a break point, etc.

[0011] Moreover, since encryption which is different when transmission media differed will be carried out, the regenerative apparatus set by it is required for the contents information enciphered by the peculiar method according to a transmission-medium system. For example, since it is enciphered by the method by which the contents information acquired through the network differed from the contents information acquired from the disk, communalization of a regenerative apparatus is checked.

[0012] Furthermore, the cipher system which is hard to decode even when using which transmission medium is demanded. Generally, as for the encryption processing in the case of the disk widely distributed as a transmission medium, what has very high safety is required. On the other hand, for reproduction of an animation, the processing speed more than fixed is required in a decryption. this invention aims at obtaining the new contents transfer method and new equipment which realize the low regenerative apparatus of cost, and advanced safety and advanced processing speed obtaining the encryption system (there being interoperability) which can be early used in common between media.

[0013]

[Means for Solving the Problem] In order to solve the above-mentioned technical problem, in the contents communication-of-information method including the decryption key information including the enciphered contents information which decrypts two or more the information record media and the contents information by which encryption was carried out [aforementioned] on a seed one or more of transmitting the information record medium of a seed to a user, the informational decryption by which encryption was carried out [aforementioned] performs two or more this inventions by the specific method one or more. The information record medium of two or more sorts of one not less than which contain two or more decryption keys further enciphered by other encryption keys in the decryption key including the enciphered contents information which decrypts the information record medium of a seed, and the contents information by which encryption was carried out [aforementioned] one or more, And in the contents communication-of-information method containing the user key which decrypts the decryption key by which encryption was carried out [aforementioned] of transmitting two or more information record media of a seed one or more, the informational decryption by which encryption was carried out [aforementioned] carries out by the single method. Furthermore, in order to raise the safety of a code, when the encryption processing speed from which at least one of the aforementioned encryption is enciphered by two stages by two kinds of keys, and at least one of the aforementioned decryptions is decrypted by two stages by two kinds of keys is taken into consideration, it is performed that at least one of the aforementioned encryption uses chaos cryptography.

[0014] More, the example of a disk is given and this invention is explained to a detail. In the contents information transfer system using a master key, a title key, a disk key, a player work key, and a user key, it solves by the method of not storing a master key for the above-mentioned technical problem in a player directly by the method of double encryption. Moreover, a problem is solved by using the new key transfer method and a more nearly high-speed cipher system. [0015] explained according to a view below Drawing 2 is explanatory drawing of the system of this invention. the master keys Kp and Kq for disk manufacture (henceforth a semi-master key) defined according to the disk manufacturer while the title key (TK) and disk key (DK) which a copyright person and a copyright manager define were enciphered by the key manager as EKa and Kb (TK, DK) with master keys Ka and Kb -- EKp and Kq (TK, DK) -- ** -- it is enciphered

[0016] By the black box supplied by the key manager, a disk manufacturer decrypts the enciphered key data, and EKp and Kq (TK, DK), gets a title key and a disk key, enciphers contents information in two stages by these two keys, and records on a disk.

[0017] It combines and the title key for a decryption enciphered with the master keys Ka and Kb supplied by the key manager, a disk key, and EKa and Kb (TK, DK) are also recorded on a disk.

[0018] Moreover, EUID (PWK1-nset) which enciphered, the key, i.e., the maker ID key, for specifying the maker who manufactures the electronic circuitries (LSI etc.), or software which decrypts the master keys Ka and Kb for decrypting a title key and a disk key, and enciphered the key group (PWK1-nset), i.e., a player work key set, which collected parts for two or more above-mentioned maker by the user ID key (UID0) is doubled, and it records on a disk

[0019] As mentioned above, when the described method generally distributes contents information only by the disk to many and unspecified persons, it is suitable.

[0020] A network is used as auxiliary means, and when offering the information for decrypting the enciphered contents information which is recorded on the disk only to a specific user in a network, it carries out as follows.

[0021] The above-mentioned master keys Ka and Kb are enciphered by the maker ID key. Enciphered by the user ID key (UID0) of fixation, key groups (PWK1-nset), i.e., a player work key set, collected [two or more]. The player work key set which did not record EUID (PWK1-nset) on the disk, but was instead enciphered by the peculiar user ID key (UIDj). Efficient employment, such as common-use-izing of the contents information enciphered while only a specific user can decrypt contents information now and being able to aim at improvement in security by distributing EUIDj (PWK1-nset) to a user through a network, can be aimed at.

[0022] Although the above-mentioned disk is effective similarly even if it replaces it by broadcast or the network medium, it also becomes possible to transmit simultaneously the player work key set enciphered by the ID key (UIDj) for every user since there was no limitation in capacity unlike a disk, and EUIDj (PWK1-nset) in the case of a network. Moreover, it is also possible to replace by radio including broadcast instead of the above-mentioned network.

[0023] The means of the reproduction in this invention system is shown in drawing 3. After EUID0 (PWK1-nset) which enciphered by the user ID key (UID0) of fixation, the key group (PWK1-nset), i.e., the player work key set, which enciphered by the maker ID key and collected two or more master keys Ka and Kb reproduced from the disk, is decrypted by the system key currently beforehand recorded on the player, the decode of the master keys Ka and Kb is carried out by the maker ID key embedded to LSI etc.

[0024] Moreover, with the master key by which the decryption was carried out [above-mentioned], the decode of the title key enciphered with the master key similarly reproduced from the disk, a disk key, and EKa and Kb (TK, DK) is carried out, and they can obtain a disk key and a title key. In this way, by the taken-out disk key and the title key, two stages of contents information doubled in encryption processing are decrypted, and contents information, such as an image and music, is reproduced.

[0025] Moreover, from a network terminal, the player work key set and EUIDj (PWK1-n) which were enciphered by the ID key (UIDj) for every user through the network to the specific user are transmitted to a player with a user ID key (UIDj) peculiar to a network terminal, and are used for a player instead of the user ID key of fixation. In this case, although it is not reproduced since EUID0 (PWK1-nset) enciphered by the user ID key of fixation is not recorded on a disk, the player work key set and EUIDj (PWK1-nset) which were enciphered by the ID key (UIDj) for every user transmitted from the network terminal are supplied, and contents are reproduced in the same procedure as the above below.

[0026] The key manager system in the system of this invention is shown in drawing 4. The key manager who received the title key hands a disk manufacturer the key data EKa and Kb (TK, DK) for a decryption with which it was enciphered for recording on the key data EKp and Kq (TK, DK) and the disk which were enciphered by two stages with two kinds of master keys for another black boxes for disk makers (semi-master key) from the disk key from a copyright manager, and a copyright person.

[0027] Moreover, the player work key set EUID0 (PWK1-nset) enciphered by the user ID key is passed to a disk manufacturer, or a player work key set (PWK1-nset) is passed to a network contractor.

[0028] By this invention, the code and decryption of the title key and disk key which are passed to a disk manufacturer are

done by two kinds of keys as mentioned above at two stages. Furthermore, the code and decryption of contents information are done by the title key and the disk key at two stages. Since cipher processing is performed doubly in this way, the system of this invention requires what has a speed quick as a cipher system. Moreover, it is also required that graphical data can be treated. There is chaos cryptography as one of the code methods which satisfies such a demand.

[0029]

[Embodiments of the Invention] A disk key and a title key are enciphered as Kp from a copyright person and a copyright manager by the keys Ka and Kb for a decryption, and are enciphered by the key control mechanism as EKp and Kq (TK, DK) by the key for EKa and Kb (TK, DK) disk manufacturers, and Kq, respectively.

[0030] By the black box supplied from a disk management mechanism, a disk manufacturer decrypts the enciphered key data, and EKp and Kq (TK, DK), gets the title key TK and the disk key DK, enciphers contents information in two stages by these two keys, and writes in a disk. About a disk key and a title key, the enciphered key data for a decryption which were passed from the key control mechanism, and EKa and Kb (TK, DK) are written in a disk. In addition, the disk key set information, EUID0 including the key Ka for a decryption, and Kb information which were enciphered (PWKI-nset) It is written in a ** disk.

[0031] Reproduction of the disk in the system of this invention is shown in drawing 3. Enciphered disk key set information EUID0 (PWKI-nset) which was read from the disk

The decode of a shell and the keys Ka and Kb for a decryption is carried out, they decrypt the enciphered key data, and EKa and Kb (TK, DK) in two stages using this key, and take out a title key and a disk key.

[0032] In this way, the taken-out contents data by which encryption processing was doubly carried out using the title key and the disk key are decrypted in two stages, and data, such as an image and an audio, are reproduced.

[0033] The key managerial system in the system of this invention is shown in drawing 4. The key data enciphered by two stages with the master key for the black boxes according to [two kinds of] disk maker, EKp and Kq (TK, DK) and the key data for a decryption, and EKa and Kb (TK, DK) cross the control mechanism which received the title key to a disk manufacturer from the disk key from a copyright manager, and a copyright person.

[0034] It is enciphered using the ID key classified by LSI maker, and the key Ka for a decryption, the enciphered disk key set information including Kb information, and EUID0 (PWKI-nset) are crossed to a disk manufacturer.

[0035] there is a chaos cipher system as one of a part of this invention or the cipher systems which can all come out of and which can be used. The procedure of the method of a chaos code is shown in drawing 5 below. The procedure of chaos cryptography used by the system of this invention is shown in drawing 5. The plaintext (information on a dimension) which consists of a key with which the user was specified, and a digital signal is transmitted to a chaos code system, and an encryption signal sentence is obtained inside this system by adding at a stream the chaos signal generated by the key to a plaintext per character. If the same key and an encryption signal sentence are transmitted to a chaos code system when decoding, a plaintext can be obtained by the same principle.

[0036] Chaos (Chaos) It is Greek meaning **** and is the phenomenon which looks irregularly and ***** like the turbulent flow of the flow of air. Unlike a random phenomenon, it can be called the complexity under an easy rule. It has the property of "it depends to initial value sensitively", "*****", "not stopping a moment, either", etc. Drawing 6 is a graph which shows the time series wave of the chaos function called logistic map.

[0037] The principle of chaos cryptography is explained. It is [plaintext / used as input data / sentence / signal / P (i) and] Chv about K (j) and a chaos signal in C (i) and a key. It is referred to as (i).

[0038] What processes P() and C() per byte, the character string (for example, a-z, 0-9) which the length becomes from an ASCII code about K() as n bytes, and its length is set to m. That is, it considers as $0 < i \leq n$ and $0 < j \leq m$. The encryption procedure of this invention is shown in drawing 7, and decryption procedure is shown in drawing 8.

[0039] About digital chaos signal generation function Chv(), it is possible to change with various kinds of chaos functions. For example, the chaos function called logistic map can be defined as follows.

Ch1(n, p) begin $X_{n+1} = p * X_n (1.0 - X_n)$ return (X_{n+1}) end [0040] Moreover, if it is a chaos function in a repeat formula, a definition can be given as follows.

Ch2(n and p) begin $X_{n+1} = X_{n-2} - \text{preturn end } ((X_{n+1} + 2.0) / 4.0)$ [0041] By the key processing module, as shown in following f(), it puts on a register by using as the code key K the character string of the arbitrary length by whom the user was inputted, and the number v of the chaos function which it is going to use out of two or more chaos functions to prepare is decided using this K, and the initial value init of the chaos function, delay delay of a chaos signal, and the parameter p of a chaos function (plurality is also possible) are decided simultaneously.

[0042]

It is the positive integer of f(K) begin job > D. = (double) (K) / Linit = job - (long int) delay (job) = (job (long int)) mod Bp = delay / L - (long int) (delay / L) v = (int) (delay / L) For a certain irrational number (for example, values, such as $L = \pi$, are also used) and D, mod Dend, however L are the number of the chaos function to prepare, and B.

[0043] The system using multi-key multiplex chaos can be constituted by using in series the algorithm mentioned above, as shown in basic parts, then drawing 9. By the system of this invention, it becomes a safer system by using this technique. To drawing 10 The sample of the plaintext by which decode was carried out to the sample of a plaintext and drawing 11 at the sample of the cipher by chaos cryptography and drawing 12 is shown.

[0044] If a key is not known by the decryption technique used now, it is impossible to decode a chaos code. Moreover, like this invention, if the system using multi-key multiplex chaos is adopted, it will become safety more. Since a chaos function can furthermore be replaced, the rule of encryption processing can be updated at any time. Furthermore, since it is a variable length key, the space (combination number) of a key increases more.

[0045] That is, it is the same. In the case of a fixed-length key, it is in the key of n figure m ***** : In the case of mn variable-length key: [0046]

[Equation 1]

$$m^n + \sum_{i=1}^{n-1} m^{n-i}$$

[0047] There is ***** . Since generating of a chaos signal carries out in stream quickly in a signal unit which is referred to as that encryption of a signal and processing of decode add a chaos signal to every [instead of a block unit / of a signal / a byte] since it is stream-processing, it can transmit and receive continuously. According to chaos cryptography, it can respond also to a high-speed optical-transmission method.

[0048] Since it is a digital formula, and it will end if only an encryption key is used, and the reference signal of the chaos signal by the side of a decoder is not needed, and it is not influenced by the noise in an information transmission but the merits and demerits of a key can be freed, a user can balance the facilities and safety easily.

[0049] In a chaos cipher system, the merits and demerits of the plaintext made into the object of security are free, and since it can respond also to what kinds, such as a text, a binary, and a graphic, of plaintexts, also in the system using graphical data, it can mainly be used satisfactory.

[0050]

[Effect of the Invention] Since according to this invention various meanses of communication of information, such as a disk, a network, and a broadcast medium, are united and distribution of efficient contents information can be aimed at, there is an effect of the cost concerning distribution being mitigated and also being able to mitigate the burden to a user's regenerative apparatus by adoption of the unified contents information scrambling system.

[0051] Moreover, according to the system of this invention, since encryption processing of a disk key and the title key is carried out doubly, the parenchyma top of decode becomes impossible. Moreover, since cipher processing also of the contents is carried out doubly, safety is increasing further. Especially, it is high speed and the burden to hardware becomes small by use of the high chaos cryptography of safety. In addition, safety increases further by taking in the processing doubly enciphered also to the managerial system of a key.

[Translation done.]

* NOTICES *

Japan Patent Office is not responsible for any damages caused by the use of this translation.

1. This document has been translated by computer. So the translation may not reflect the original precisely.
2. **** shows the word which can not be translated.
3. In the drawings, any words are not translated.

DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]

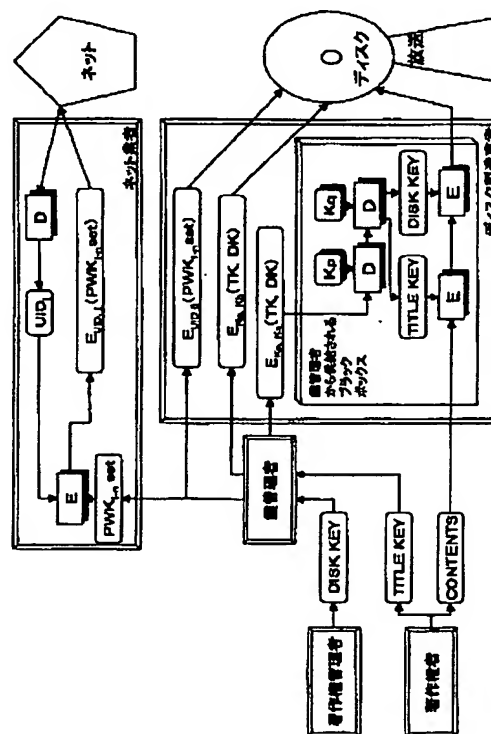
- [Drawing 1] It is outline explanatory drawing of the contents information encryption in a disk.
- [Drawing 2] It is outline explanatory drawing of creation of the disk in the system of this invention.
- [Drawing 3] It is outline explanatory drawing about reproduction of the disk in the system of this invention.
- [Drawing 4] It is outline explanatory drawing of the key managerial system in the system of this invention.
- [Drawing 5] It is the conceptual diagram of a chaos cipher system.
- [Drawing 6] It is the time series wave of logistic map chaos.
- [Drawing 7] It is the flow diagram of the encryption procedure of chaos cryptography.
- [Drawing 8] It is the flow diagram of the decryption procedure of chaos cryptography.
- [Drawing 9] It is the conceptual diagram of the multi-key multiplex chaos encryption system of chaos cryptography.
- [Drawing 10] It is the sample of a plaintext.
- [Drawing 11] It is the sample of the cipher by chaos cryptography.
- [Drawing 12] It is the sample of the plaintext by which decode was carried out.
-

[Translation done.]

(11)特許出願公開番号

(43)公開日 平成11年(1999)10月15日

659



【特許請求の範囲】

【請求項1】暗号化されたコンテンツ情報を含む1以上複数種の情報記録媒体、および前記暗号化されたコンテンツ情報を復号化する復号化キー情報を含む1以上複数種の情報記録媒体をユーザーに伝達するコンテンツ情報伝達方法において、前記暗号化された情報の復号化が単一の方法で行われることを特徴とするコンテンツ情報伝達方法。

【請求項2】暗号化されたコンテンツ情報を含む1以上複数種の情報記録媒体、前記暗号化されたコンテンツ情報を復号化する復号化キーを他の暗号化キーでさらに暗号化された復号化キーを含む1以上複数種の情報記録媒体、および前記暗号化された復号化キーを復号化するユーザーIDキーを含む1以上複数種の情報記録媒体を伝達するコンテンツ情報伝達方法において、前記暗号化された情報の復号化が単一の方法で行われることを特徴とするコンテンツ情報伝達方法。

【請求項3】前記暗号化のうち少なくとも一つが2種類のキーで2段階に暗号化され、前記復号化のうち少なくとも一つが2種類のキーで2段階に復号化されることを特徴とする請求項1または2記載のコンテンツ情報伝達方法。

【請求項4】前記暗号化のうち少なくとも一つがカオス暗号法を用いて、2種類のキーで2段階に暗号化され、前記復号化が2種類のキーで2段階に復号化されることを特徴とする請求項1または2記載のコンテンツ情報伝達方法。

【請求項5】暗号化されたコンテンツ情報を含む1以上複数種の情報記録伝達手段、および前記暗号化されたコンテンツ情報を復号化する復号化キー情報を含む1以上複数種の情報記録伝達手段を備えたコンテンツ情報伝達システムにおいて、前記暗号化された情報の復号化が特定の手段で行われることを特徴とするコンテンツ情報伝達システム。

【請求項6】暗号化されたコンテンツ情報を含む1以上複数種の情報記録伝達手段、前記暗号化されたコンテンツ情報を復号化する復号化キーを他の暗号化キーでさらに暗号化された復号化キーを含む1以上複数種の情報記録伝達手段、および前記暗号化された復号化キーを復号化するユーザーIDキーを含む複数種の1以上複数種の情報記録伝達手段を備えたコンテンツ情報伝達システムにおいて、前記暗号化された情報の復号化が特定の手段で行われることを特徴とするコンテンツ情報伝達システム。

【請求項7】前記暗号化のうち少なくとも一つが2種類のキーで2段階に暗号化される手段、前記復号化のうち少なくとも一つが2種類のキーで2段階に復号化される手段を備えたことを特徴とする請求項5または6記載のコンテンツ情報伝達システム。

【請求項8】前記暗号化のうち少なくとも一つがカオス

暗号法を用いて、2種類のキーで2段階に暗号化される手段、前記復号化が2種類のキーで2段階に復号化される手段を備えたことを特徴とする請求項5または6記載のコンテンツ情報伝達システム。

【発明の詳細な説明】**【0001】**

【発明の属する技術分野】本発明は情報伝送におけるコンテンツ情報およびコンテンツ情報を暗号化するキーの暗号化に関する。

【0002】

【従来の技術】従来、コンテンツ情報などを伝えるにあたって、伝達手段としてディスクやテープなどのパッケージ媒体、ネットワークなどの有線通信媒体、地上放送、衛星放送・通信などの無線放送・通信媒体）が用いられている。これらの媒体を使って送られるコンテンツ情報は、それぞれの媒体に応じて固有の暗号化処理（スクランブル処理）が行われている。

【0003】例えば、ディスクに記録されたコンテンツ情報が映像情報が暗号化されたデータであれば、その記録されたデータを読み出したり、コピーしても、データを復号化するキーがない限り再生できない。このような暗号化によってディスクの不正コピーや著作権者の意図しない使用方法が阻止される。

【0004】暗号解除処理は通常、専用LSIを使って行われることが多いが、汎用コンピュータによってソフトウェアで行うことも可能である。しかし、いずれの方法を採るにしても、デバグやアセンブル・ツールなどを使って解析できないようにすることが必要である。このような内部解析を防ぐ「耐性」を備えたソフトウェアはタンパーレジストソフトウェア（Tamper Resistant Software）と呼ばれている。

【0005】ディスクにおけるコンテンツ情報暗号化の一例の概略を図1に示す。中立的立場にある鍵管理者が保持するマスターキーと、著作権者などが定めるディスクキーおよび著作権者が管理するタイトルキーを階層的に組み合わせてコンテンツ情報を暗号化する。

【0006】マスターキーは、例えば暗号解除用LSIや復号化ソフトウェアメーカーごとに異なる暗号化キーである。鍵管理者はこれらのマスターキーを一括して管理する。ディスクキーは映画会社や音楽会社などの著作権管理者が管理し、タイトルキーは著作権者や著作権者に代わって著作権管理者が管理する。ディスクキーはディスク1枚に一つ設定され、タイトルキーはタイトル毎や、著作権者に合わせて複数設定されても良い。ディスクキーはマスターキーを使って暗号化する。専用LSIで復号化する場合、キーデータやアルゴリズムなどはLSIの内部構造によって隠蔽される。

【0007】ディスクキーを暗号化するときはLSIメーカー毎の異なったマスターキーでも復号化できるようなディスクキーセットを作ってディスクに記録しておく。

暗号化されたマスターキーによって暗号化されたディスクキーとディスクキーによって暗号化されたタイトルキーはタイトルキーによって暗号化されたコンテンツ情報と共にディスクに記録される。いずれのキーも暗号化されているので、コンテンツ情報の復号化に必要なタイトルキーを知ることはいかなる。

【0008】

【発明が解決しようとする課題】コンテンツ情報がディスク、暗号キーが通信で送られてくるような場合は、それぞれ独自の方式で暗号化がなされていることが多く、復号化処理は複数種類用意しなければならない。このため、再生装置は複数種の復号化手段を備えるために、装置が複雑化し、コストが上昇する。また、装置を簡易化すると、暗号の安全性の面で問題が出てくる。

【0009】図1に示したように、従来のディスクの暗号化方式では、コンテンツ情報をタイトルキーで、タイトルキーをディスクキーで、ディスクキーをマスターキーでそれぞれ暗号化するという直列的なパターンである。暗号の不正解読者が、タイトルキーだけに「全数キー探索」の方法で攻撃すれば、特に鍵の長さが制限がある場合、有限の時間内で解読できるので、安全強度が全然足りない。例えば、暗号キーが40 bitならば、数時間内で解読できるので、著作権を有効に守ることができない。また、従来の暗号化方式では、マスターキーをそのままプレーヤーの中に格納することになるので、解読者に探される可能性があり、非常に危険である。

【0010】ディスクシステムで用いられる暗号化方式は三つの暗号化キーデータやこれらの復号化アルゴリズム、パス認証のアルゴリズムなどの情報を持っている。これらの秘密情報をリバースエンジニアリングから守るために、ソフトウェアやデバッグや、スナップショット解析、ブレークポイントの設定などに対処する必要がある。

【0011】また、伝送媒体システムに合わせて固有の方式で暗号化されるコンテンツ情報は、伝送媒体が異なれば異なった暗号化がされることになるので、それに合わせた再生装置が必要である。例えばネットワークを通して得たコンテンツ情報とディスクから得たコンテンツ情報が異なった方式で暗号化されているので、再生装置の共通化が阻害される。

【0012】さらに、いずれの伝送媒体を使用する場合でも解読されにくい暗号方式が要求されている。一般に、伝送媒体として広く頒布されるディスクの場合の暗号化処理はきわめて安全性の高いものが要求される。一方、動画の再生のためには復号化において一定以上の処理速度が要求される。本発明は、コストの低い再生装置を実現する新たなコンテンツ伝達方法および装置を得ること、および高度の安全性と処理速度が早く、媒体間で共通に使用できる（インターオペラビリティのある）暗号化システムを得ることを目的とする。

【0013】

【課題を解決するための手段】本発明は上記課題を解決するために、暗号化されたコンテンツ情報を含む1以上複数種の情報記録媒体、および前記暗号化されたコンテンツ情報を復号化する復号化キー情報を含む1以上複数種の情報記録媒体をユーザーに伝達するコンテンツ情報伝達方法において、前記暗号化された情報の復号化が特定の方法で行う。暗号化されたコンテンツ情報を含む1以上複数種の情報記録媒体、前記暗号化されたコンテンツ情報を復号化する復号化キーを他の暗号化キーでさらに暗号化された復号化キーを含む1以上複数種の情報記録媒体、および前記暗号化された復号化キーを復号化するユーザーキーを含む1以上複数種の情報記録媒体を伝達するコンテンツ情報伝達方法において、前記暗号化された情報の復号化が単一の方法で行う。さらに、暗号の安全性を高めるために、前記暗号化のうち少なくとも一つが2種類のキーで2段階に暗号化され、前記復号化のうち少なくとも一つが2種類のキーで2段階に復号化される暗号化処理速度を考慮した場合は、前記暗号化のうち少なくとも一つがカオス暗号法を用いることが行われる。

【0014】本発明をより詳細にディスクの例を挙げて説明する。マスターキー、タイトルキー、ディスクキー、プレーヤーワークキー、ユーザーキーを用いるコンテンツ情報伝達システムにおいて、2重暗号化の方法で上記課題を、マスターキーを直接にプレーヤーの中に格納しない方法で解決する。また、新たなキー転送方法およびより高速な暗号方式を使うことで問題を解決する。以下図に示したがって説明する。

【0015】図2は本発明のシステムの説明図である。著作権者や著作権管理者が定めるタイトルキー（TK）、ディスクキー（DK）は鍵管理者によってマスターキー K_a 、 K_b により、 $E_{K_a, K_b}(TK, DK)$ と暗号化されると共にディスク製造業者別に定められたディスク製造用マスターキー（以下準マスターキーと云う） K_p 、 K_q により、 $E_{K_p, K_q}(TK, DK)$ へと暗号化される。

【0016】ディスク製造業者は鍵管理者から供給されるブラックボックスにより、暗号化されたキーデータ、 $E_{K_p, K_q}(TK, DK)$ を復号化してタイトルキーとディスクキーを得て、この2つのキーでコンテンツ情報を2段階に暗号化してディスクに記録する。

【0017】併せて、鍵管理者から供給されるマスターキー K_a 、 K_b により暗号化された復号化用のタイトルキーとディスクキー、 $E_{K_a, K_b}(TK, DK)$ もディスクに記録する。

【0018】またタイトルキーとディスクキーを復号化するためのマスターキー K_a, K_b を、復号化する電子回路（LSIなど）と／あるいはソフトを製造するメーカーを特定するためのキーすなわちメーカーIDキーによって暗号化し、複数の上記メーカー分を集めたキー群すなわちプレーヤワークキーセット($PWK_{1-n}set$)をユーザーIDキー（UID0）で暗号化した、

$E_{UID}(PWK_{1-n}set)$

を合わせてディスクに記録する。

【0019】以上、述べた方法は一般的には不特定多数に対してディスクのみでコンテンツ情報を配信する場合に適している。

【0020】ネットワークを補助手段として使用し、ディスクに記録されている暗号化されたコンテンツ情報を復号化するための情報をネットワークで特定のユーザーに対してのみに提供する場合は以下のように行う。

【0021】上記マスターキー K_a, K_b をメーカーIDキーによって暗号化し、複数集めたキー群すなわちプレーヤワークキーセット($PWK_{1-n}set$)を固定のユーザーIDキー（UID0）で暗号化した、

$E_{UID}(PWK_{1-n}set)$

をディスク上には記録せず、代わりに固有のユーザーIDキー（UIDj）で暗号化したプレーヤワークキーセット、

$E_{UIDj}(PWK_{1-n}set)$

をネットワークを介してユーザーに配信することによって特定ユーザーのみがコンテンツ情報を復号化できるようになり、セキュリティの向上が図れると共に暗号化されたコンテンツ情報の共用化等効率的な運用が図れる。

【0022】上記ディスクは放送やネットワーク媒体で置き換えても同様に有効であるが、ネットワークの場合にはディスクと異なり容量に限界がないのでユーザー毎のIDキー（UIDj）で暗号化されたプレーヤワークキーセット、

$E_{UIDj}(PWK_{1-n}set)$

を同時に伝送することも可能になる。また、上記ネットワークの代わりに放送をはじめとした無線通信で置き換えることも可能である。

【0023】本発明システムにおける再生の手段を図3に示す。ディスクから再生された、マスターキー K_a, K_b をメーカーIDキーによって暗号化し複数集めたキー群すなわちプレーヤワークキーセット($PWK_{1-n}set$)を固定のユーザーIDキー（UID0）で暗号化した、

$E_{UID0}(PWK_{1-n}set)$

はあらかじめプレーヤに記録されているシステムキーで復号化された後、LSI等に埋め込まれたメーカーIDキーによってマスターキー K_a, K_b が復号される。

【0024】また同じくディスクから再生されたマスターキーによって暗号化されたタイトルキー、ディスクキー、

$E_{K_a, K_b}(TK, DK)$

は、上記復号化されたマスターキーによって復号され、ディスクキーとタイトルキーをえることができる。こうして取り出されたディスクキーとタイトルキーによって2重に暗号化処理をされたコンテンツ情報を2段階復号化して映像や音楽などのコンテンツ情報を再生する。

【0025】また、特定ユーザーに対してネットワークを介してユーザー毎のIDキー（UIDj）で暗号化されたプレーヤワークキーセット、

$E_{UIDj}(PWK_{1-n})$

はネットワーク端末からプレーヤにネットワーク端末固有のユーザーIDキー（UIDj）と共にプレーヤに転送され、固定のユーザーIDキーの代わりに使用される。この場合ディスクには固定のユーザーIDキーで暗号化した、

$E_{UID0}(PWK_{1-n}set)$

が記録されていないので再生されないが、ネットワーク端末から転送されたユーザー毎のIDキー（UIDj）で暗号化されたプレーヤワークキーセット、

$E_{UIDj}(PWK_{1-n}set)$

が供給されて以下上記と同様の手順でコンテンツが再生される。

【0026】本発明のシステムにおける鍵管理者システムを図4に示す。著作権管理者からディスクキー、著作権者からタイトルキーを受け取った鍵管理者は2種類のディスクメーカー用別ブラックボックス用マスターキー（準マスターキー）で2段階に暗号化されたキーデータ

$E_{K_p, K_q}(TK, DK)$

およびディスクに記録するための暗号化された復号化用キーデータ

$E_{K_a, K_b}(TK, DK)$

をディスク製造業者に渡す。

【0027】また、ユーザーIDキーで暗号化されたプレーヤワークキーセット

$E_{UID0}(PWK_{1-n}set)$

をディスク製造業者に渡すかあるいはプレーヤワークキーセット($PWK_{1-n}set$)をネットワーク業者に渡す。

【0028】本発明では上記のように、ディスク製造業者に渡すタイトルキー及びディスクキーを2種類のキーで2段階に暗号・復号化する。さらに、コンテンツ情報をタイトルキー及びディスクキーで2段階に暗号・復号化する。本発明のシステムではこのように、2重に暗号処理を行っているため、暗号方式としては速度の速いものが要求される。また、グラフィックデータを扱えることも要求される。このような要求を満足する暗号方法の一つとしてはカオス暗号法がある。

【0029】

【発明の実施の形態】著作権者および著作権管理者からディスクキーとタイトルキーは、鍵管理機構により、復号化用キー K_a, K_b により

$E_{K_a, K_b}(TK, DK)$

ディスク製造業者用のキー、 K_p, K_q により

$E_{Kp, Kq}$ (TK, DK)

とそれぞれ暗号化される。

【0030】ディスク製造業者はディスク管理機構から供給されるブラックボックスにより、暗号化された鍵データ、

$E_{Ka, Kb}$ (TK, DK)

を復号化してタイトルキーTKとディスクキーDKを得て、この2つのキーでコンテンツ情報を2段階に暗号化してディスクに書き込む。ディスクキーとタイトルキーについては、鍵管理機構から渡された暗号化された復号化用キーデータ、

$E_{Ka, Kb}$ (TK, DK)

をディスクに書き込む。この他に、復号化用キーKa、Kb情報を含む暗号化されたディスクキーセット情報、

E_{UID0} (PWK_{1-n}set)

がディスクに書き込まれる。

【0031】本発明のシステムにおけるディスクの再生を図3に示す。ディスクから読み出された暗号化されたディスクキーセット情報

E_{UID0} (PWK_{1-n}set)

から、復号化用キーKa、Kbが復号され、このキーを用いて、暗号化されたキーデータ、

$E_{Ka, Kb}$ (TK, DK)

を2段階に復号化し、タイトルキーとディスクキーを取り出す。

【0032】こうして取り出された、タイトルキーとディスクキーを用いて、2重に暗号化処理されたコンテンツデータを2段階に復号化して映像、オーディオなどのデータを再生する。

【0033】本発明のシステムにおける鍵管理システムを図4に示す。著作権管理者からディスクキー、著作権者からタイトルキーを受け取った管理機構は、2種類のディスクメーカー別ブラックボックス用マスターキーで2段階に暗号化された鍵データ、

$E_{Kp, Kq}$ (TK, DK)

および、復号化用キーデータ、

$E_{Ka, Kb}$ (TK, DK)

がディスク製造業者に渡る。

【0034】復号化用キーKa、Kb情報を含む暗号化されたディスクキーセット情報、

E_{UID0} (PWK_{1-n}set)

はLSIメーカー別IDキーを用いて暗号化され、ディスク製造業者に渡る。

【0035】本発明の一部あるいは全部で用いることができる暗号化方式の一つとしてカオス暗号化方式がある。以下カオス暗号化方式の手順を図5に示す。本発明のシステムで用いられるカオス暗号化方式の手順を図5に示す。使用者の指定された鍵とデジタル信号からなる平文（元の情報）をカオス暗号システムに伝送して、本システムの内部ではその鍵によって発生されたカオス信号を平文

に文字単位でストリームに付加することで、暗号化信号文を得る。復号するとき、同様な鍵と暗号化信号文をカオス暗号システムに伝送すれば、同様の原理で平文を得られる。

【0036】カオス(Chaos)は混沌を意味するギリシャ語であり、空気の流れの乱流のように不規則、予測不可能に見える現象である。ランダム現象とは違い、簡単な規則の下での複雑さといえる。「初期値に敏感に依存する」、「予測不可能」、「一刻でも停止しない」などの特性を有する。図6はロジスティック写像と呼ばれるカオス関数の時系列波形を示すグラフである。

【0037】カオス暗号法の原理について説明する。入力データとなる平文をP(i)、信号文をC(i)、鍵をK(j)、カオス信号をChv(i)とする。

【0038】P(i)とC(i)をバイト単位で処理するもの、その長さはnバイトとして、K(i)をアスキーコードからなる文字列（例えば、a~z, 0~9）、その長さはmとする。即ち、

$$0 < i \leq n, 0 < j \leq m$$

とする。本発明の暗号化手続きを図7に、復号化手続きを図8に示す。

【0039】デジタルカオス信号発生関数Chv(i)については、各種のカオス関数で入れ替えることが可能である。例えば、ロジスティック写像と呼ばれるカオス関数を次のように定義できる。

Ch1(n, p)

begin

$$X_{n+1} = p * X_n (1.0 - X_n)$$

return (X_{n+1})

end

【0040】また、繰り返し公式によるカオス関数ならば次のように定義できる。

Ch2(n, p)

begin

$$X_{n+1} = X_n^2 - p$$

$$\text{return } ((X_{n+1} + 2.0) / 4.0)$$

end

【0041】キー処理モジュールでは下記のf(i)に示すように、ユーザの入力された任意長の文字列を暗号キーKとしてレジスタに置き、このKを用い、準備しておく複数のカオス関数の中から使用しようとするカオス関数の番号vを決め、また、そのカオス関数の初期値init、カオス信号の遅れdelay、及びカオス関数のパラメータp（複数も可能）を同時に決める。

【0042】

f(K)

begin

$$\text{job} = (\text{double})(K) / L$$

$$\text{init} = \text{job} - (\text{long int})(\text{job})$$

$$\text{delay} = (\text{long int})(\text{job}) \bmod B$$

```

p    =delay/L-(long int)(delay/L)
v    =(int)(delay/L) mod D
end

```

ただし、Lはある無理数（例えば、 $L=\pi$ などの値も用いられる）、Dは準備しておくカオス関数の個数、Bは $> D$ の正整数である。

【0043】上述したアルゴリズムを基本部品とすれば、図9に示すように直列に利用することによって、多鍵多重カオスを用いたシステムを構成することができる。本発明のシステムではこの手法を利用することで、より安全なシステムとなる。図10に 平文のサンプル、図11にカオス暗号法による暗号文のサンプル、図12に復号された平文のサンプルを示す。

【0044】現在使われている暗号解説手法では、鍵が分からないとカオス暗号を解説することが不可能である。また、本発明のように、多鍵多重カオスを用いたシステムを採用すれば、より安全になる。さらにカオス関数は入れ換えることができるので暗号化処理のルールはいつでも更新できる。さらに、可変長鍵であるから、鍵の空間（組み合わせ個数）はより多くなる。

【0045】即ち、同様の n 桁 m 進数値の鍵には、固定長鍵の場合： m^n

可変長鍵の場合：

【0046】

【数1】

$$m^n + \sum_{i=1}^{n-1} m^{n-i}$$

【0047】の組み合わせがある。カオス信号の発生は速く、かつ、ストリーミ的な処理であるから、信号の暗号化と復号の処理は、ブロック単位ではなく、信号のバイトずつにカオス信号を付加するというような信号単位でストリーミ的に行うから、連続的に送受信できる。カオス暗号法によれば高速な光伝送方式にも対応することができる。

【0048】デジタル式であるから、暗号化鍵だけを使用すれば済み、復号器側のカオス信号の参照信号はいらないし、情報伝送中のノイズには影響されず、鍵の長短は自由にすることができるので、ユーザはその便利さと安全のバランスを簡単に取ることができる。

【0049】カオス暗号方式では機密保護の対象とする

平文の長短は自由であり、テキスト、バイナリ、グラフィックなどのどんな種類の平文にも対応できるので、主にグラフィックデータを使うシステムにおいても問題なく使用できる。

【0050】

【発明の効果】本発明によれば、ディスク、ネットワーク、放送媒体などの各種情報伝達手段を融合して効率的なコンテンツ情報の配信がはかれるので、配信に係わるコストを軽減でき、統一されたコンテンツ情報スクランブリングシステムの採用によりユーザーの再生装置に対する負担も軽減できるなどの効果がある。

【0051】また、本発明のシステムによれば、ディスクキー及びタイトルキーは2重に暗号化処理されているので、解説は実質上不可能となる。また、コンテンツも二重に暗号化処理されているのでさらに安全性が高まっている。とくに、高速でかつ安全性の高いカオス暗号法の利用により、ハードウェアへの負担が小さくなる。そのほかに、鍵の管理システムにも二重に暗号化する処理を取り入れることにより安全性がさらに高まる。

【図面の簡単な説明】

【図1】ディスクにおけるコンテンツ情報暗号化の概略説明図である。

【図2】本発明のシステムにおけるディスクの作成の概略説明図である。

【図3】本発明のシステムにおけるディスクの再生を概略説明図である。

【図4】本発明のシステムにおける鍵管理システムの概略説明図である。

【図5】カオス暗号化方式の概念図である。

【図6】ロジスティック写像カオスの時系列波形である。

【図7】カオス暗号法の暗号化手続きのフロー・ダイアグラムである。

【図8】カオス暗号法の復号化手続きのフロー・ダイアグラムである。

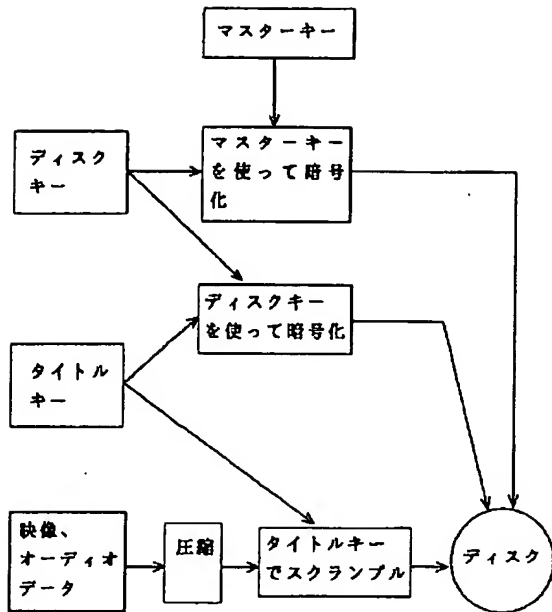
【図9】カオス暗号法の多鍵多重カオス暗号化システムの概念図である。

【図10】平文のサンプルである。

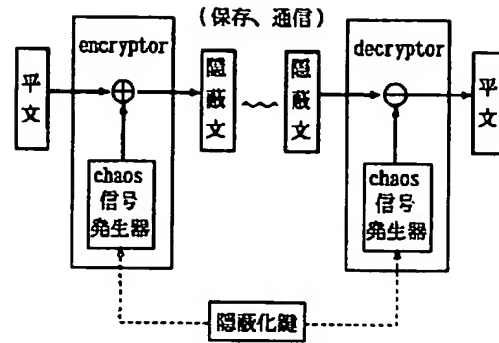
【図11】カオス暗号法による暗号文のサンプルである。

【図12】復号された平文のサンプルである。

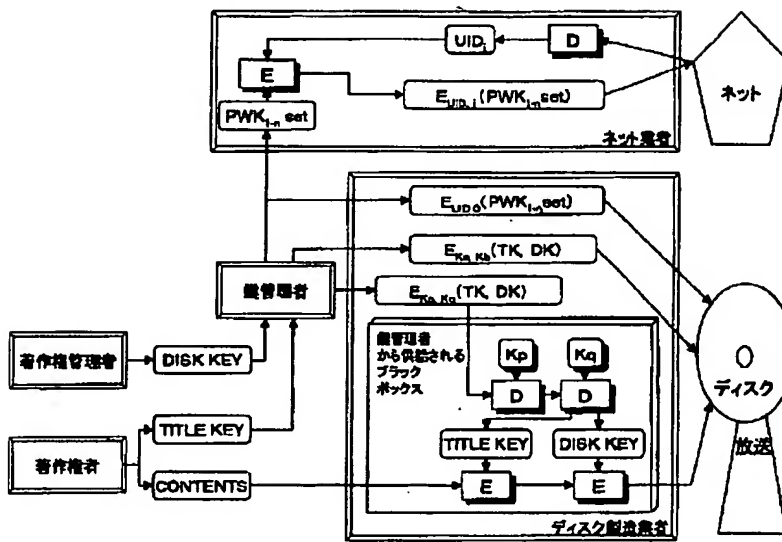
【図1】



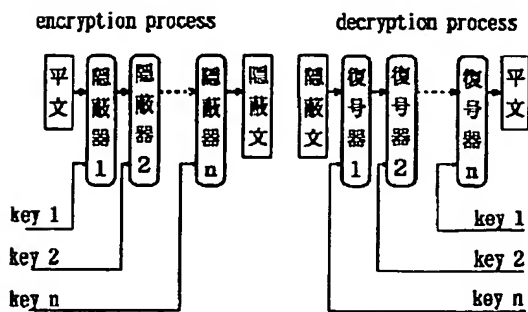
【図5】



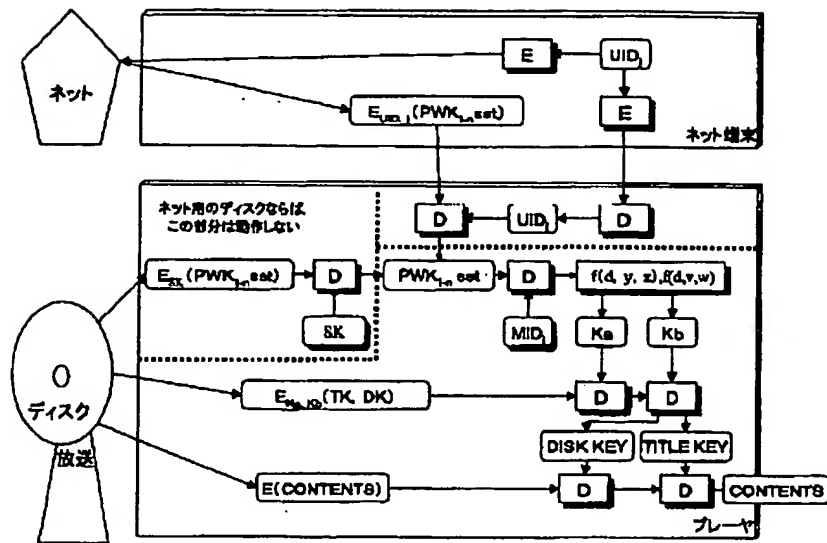
【図2】



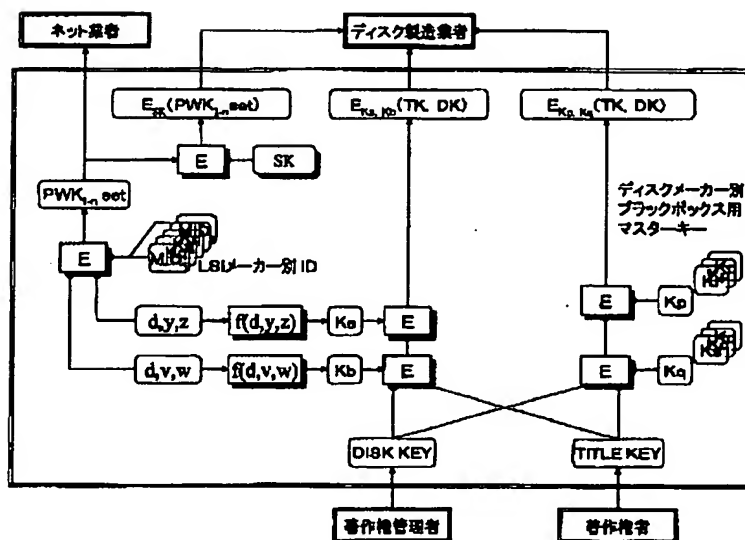
【図9】



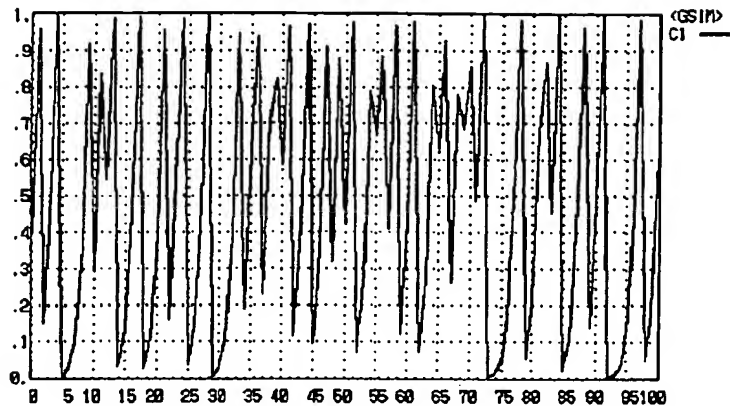
【図3】



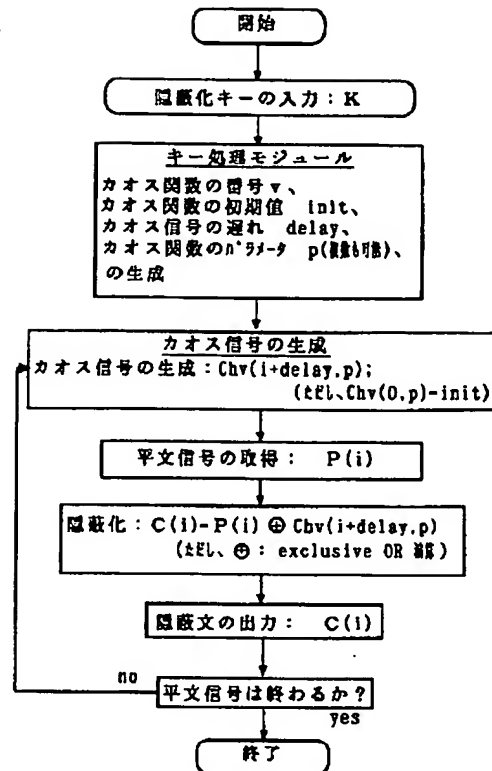
【図4】



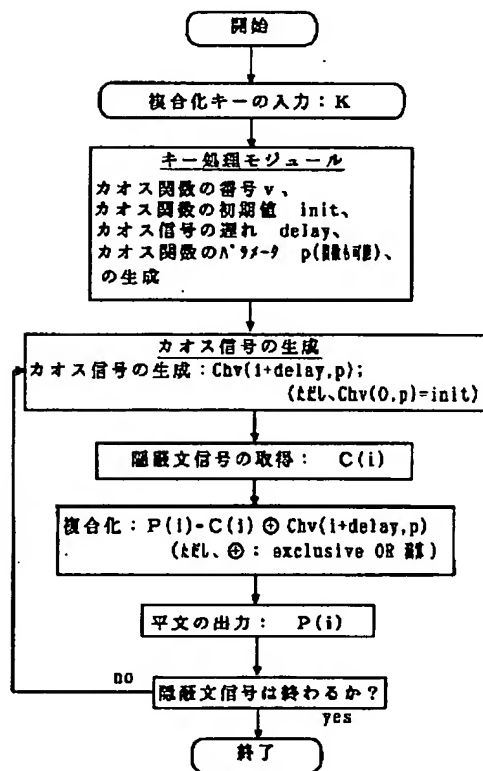
【図6】



【図7】



【図8】



【図10】

[illegible]

【图 1 2】

[illegible]